The right item, right place, right time.

Privacy Act 201
Collecting Personal Data

Who Needs to Take This Training?

This training is designed for the DLA Workforce who:

- Design Databases
- Maintain or Post Data to Web Sites
- Design Forms or Surveys

-- AND --

- Anyone Requesting the Services of these Professionals
- Anyone Supervising these Professionals

Why Some Professionals Need Targeted Privacy Act Training

- Data collection is an integral part of recordkeeping in DOD.
- You design and/or maintain the systems, forms, and surveys used to gather and store personal information.
- It is vital that you have a working knowledge of the Privacy Act.
- But most importantly, the Privacy Act requires it!

The Privacy Act Impacts Design

- The Privacy Act Controls:
  - What data elements you may collect and store
  - How data is to be safeguarded
  - Who may be granted access

You Must Know
Two Key Privacy Act Terms

- "System of records" AND "System of records notice"

- A "system of records" is a group of files that:

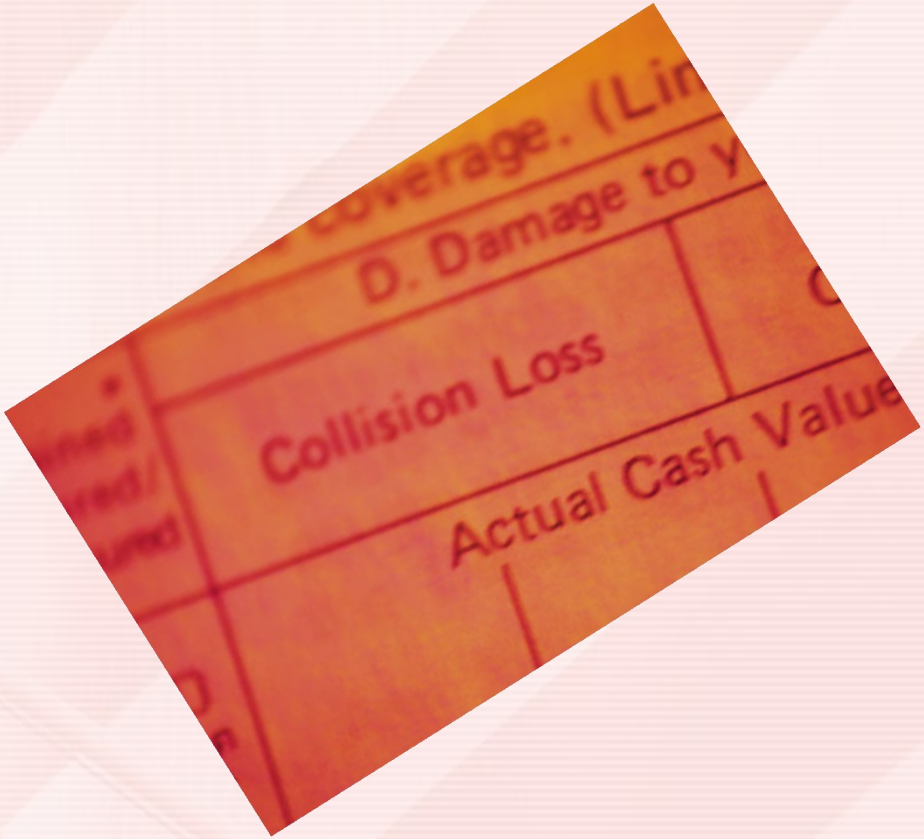
  - Contains a personal identifier (such as a name, date of birth, Social Security Number, Employee Number, fingerprint, etc.);
  - Contains at least one other item of personal data (such as home address, performance rating, blood type, etc.); and
  - The data about the subject individual **IS** retrieved by their personal identifier(s).

You Must Know
Two Key Privacy Act Terms

- A “system of records notice” is a formal document setting the rules for operating a Privacy Act “system of records.” The notice:
  - Is published in the *Federal Register;*
  - Advises the public of our data collections; and
  - States what data may be collected and how it will be used, stored, shared, and safeguarded.
- All DOD individuals must comply with rules listed in the notice. There may be serious **penalties** for those who ignore the rules.

Data Collection Devices

- Databases
- Forms
- Surveys & Questionnaires
- Web Sites
- Even Verbal Questions!



Designing Data Collection Devices

Before Designing a Collection Device . . .

Step 1: Verify that a System of Records Notice has been published covering your collection.

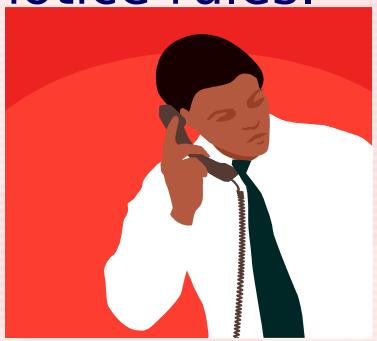
- DOD System Notices: http://www.dod.mil/privacy/notices
- Government-Wide System Notices: http://www.dod.mil/privacy/govwide

Step 2: Verify that the data elements are covered in the "Categories of Records" clause of the System of Records Notice.

Consult with your local Privacy Act Office Early and Often!

What Data Elements Are Authorized To Be Collected?

- If a Privacy Act system of records notice has **NOT** been published, consult with:
  - The Data Owner
  - The local Privacy Act Office
- A System Notice must be published **BEFORE** you begin your data collection.
- If a Privacy Act System Notice **HAS** been published:
- Review and Follow the system of records notice rules.
  - “Categories of Records”
    - Lists the Authorized Data Elements
  - “Categories of Individuals”
    - Lists the Authorized Population



Collecting Personal Data
Four Key Requirements

1. Collect the minimalist amount of personal data that is both **relevant** and **necessary** to accomplish a purpose of the agency required by federal statute or Executive Order.

2. Collect data directly from the record subject whenever possible.

3. Conduct data collections using fair and lawful means.

4. When collecting data from the individual to be maintained in a system of records, provide a Privacy Act Statement.

Privacy Act Statements & Advisories

- Required by Sections (e)(3) and 7(b) of the Privacy Act

- Use when an individual is asked -
  - To provide his SSN or other personal data.
  - To confirm that his data is current or correct.

- Allows the individual to make an informed decision about providing his data.

➢ Statements: Use when personal data will be filed within a System of Records.

➢ Advisories: Use when SSN is collected but data will not be filed in a System of Records.

Privacy Act Statements – Required Elements

- The Statement tells the individual:
  - ⇨ Your purpose.
  - ⇨ Your authority.
  - ⇨ Who outside DOD will have access to the data.
  - ⇨ Whether providing the data is mandatory or voluntary.
  - ⇨ What will happen if the individual refuses.
  - ⇨ The name, number, and an electronic link to the governing Privacy Act System Notice.

- Most of the data for the Statement is taken from the Privacy Act system notice.

Sample
Privacy Act Statement

Privacy Act Statement

Authority: 5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 6122, Flexible Schedules; E.O. 9397 (SSN); and E.O. 10450, Security Requirements for Government Employees.

Purpose: Information is collected to verify your eligibility to access DLA-controlled facilities and for issuing badges for use in entering facilities.

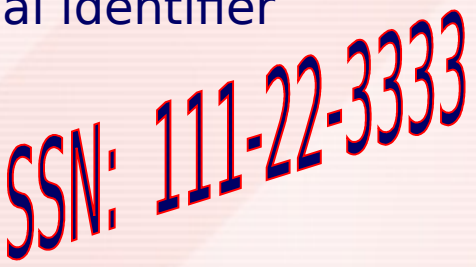
Routine Uses: Information may be disclosed for any of the DOD "Blanket Routine Uses" published at http://www.dod.mil/privacy/notices/blanket-uses.html. Contact your local DLA Privacy Act Officer for further details.

Disclosure: Voluntary; however, failure to provide the information may result in our inability to grant you access to our facilities.

Rules of Use: Rules for collecting, using, retaining, and safeguarding this information are contained in DLA Privacy Act System Notice S500.50, entitled "Facility Access Records" available at http://www.dod.mil/privacy/notices/dla.

The Privacy Act Advisory

- Use an “Advisory” when –
  - You will retrieve the data by non-personal identifier (geographic area, date, etc.) AND
  - You are collecting SSNs.



- Tell the Individual:
  - Your authority.
  - Whether disclosure is mandatory or voluntary AND
  - How you will use the SSN.
- Data for the Advisory is typically be found in the governing DOD Regulation, Directive, or Instruction.

NOTE: **If your collection device will be used Component-wide, consider using a Statement since you can’t guarantee how a field activity will retrieve the data.**

Sample Privacy Act Advisory

Privacy Act Advisory

Authority: 18 U.S.C. 1029, Access device fraud; E.O. 9397 (SSN).

Disclosure of your SSN is voluntary: However, if you fail to provide your SSN, we will be unable to grant you access to the DLA XYZ database.

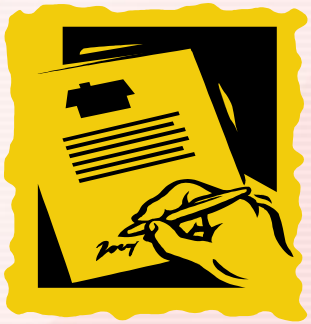
Uses to be made of your SSN: Your SSN will be compared against a master list of DLA employees for the sole purpose of positively identifying you. It will not be shared with anyone outside DOD. Once we have confirmed your identity, we will destroy this form.

Sample

This data collection will not become part of any Privacy Act System of Records.

Sidebar: Is my Collection Voluntary or Mandatory?

- Nearly all collections are voluntary.
- Collections may be listed as “mandatory” only if--
  - The person is required by law to provide the data AND
  - The person is subject to penalty for refusing.
- If providing the data is only a condition of granting a benefit and the individual has the option of requesting that benefit, then the collection is voluntary.



Consult with your Privacy Act Officer and Counsel before listing <u>any</u> collection as mandatory.

Where do I Place the Privacy Act Statement or Advisory?

For Forms: Preferably at top of page immediately under the title of the form.

For Surveys: Opening page of survey OR in a cover memo appended to the survey.

For Web Pages: Conspicuously on the screen that collects the data.

For Other Locations: Boldly referenced at the top of the collection device:

Example 1:

Click Here to Read Our Privacy Act Statement

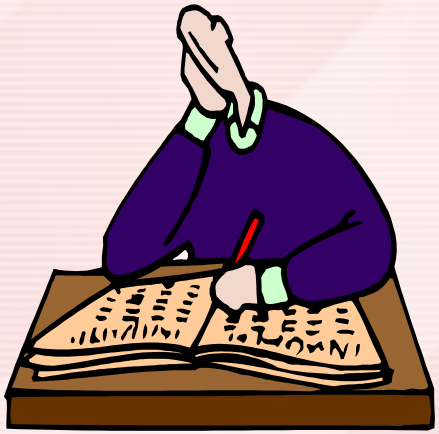
Example 2:

See Our Privacy Act Statement on Page 3.

Statements appearing as pop-ups must be in printable format.

Suppose I Use a Form Created by Another Agency or the Private Sector?

- If the form has an existing Privacy Act Statement:
  - The Statement must agree with your uses.
  - If it doesn't, attach a corrected Statement reflecting your purpose and intended uses.
- If the form carries no Statement:
  - Create one and attach it to the form.
- Use your System Notice as the source for the Statement wording.



Suppose I'm Conducting a Mass Collection or Collecting Data via Telephone?

- Mass Collections –

  Place large-print Statement on a wall where those waiting in line may read it.

- Telephone Collections –

  Have a copy of the Statement available to read to the individual upon request.

SIDEBAR
"Privacy Act Statement" vs. "Privacy and Security Notice"

Q: Is the Privacy Act Statement the same thing as the Privacy and Security Notice I see on websites?

SIDEBAR
"Privacy Act Statement" vs. "Privacy and Security Notice"

ANSWER: No – These are not the same.

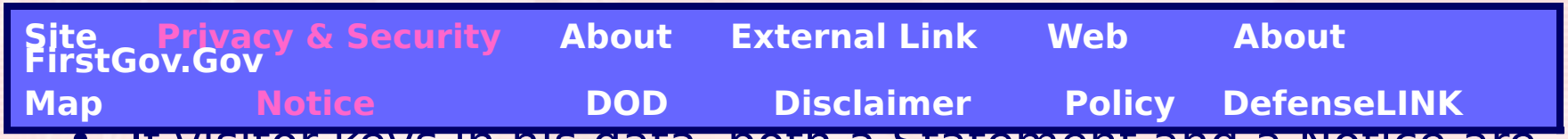
- Privacy Act Statement:
  - Used when an individual is asked to provide his personal data.
  - The individual is aware of the collection is taking place because he is providing the information.
- Privacy and Security Notice:
  - Used when your Web site automatically collects data from visitors to your site.
  - The visitor is unaware that the collection is occurring.

If your Web site asks visitors to key in their personal data, both a Privacy Act Statement and a Privacy and Security Notice will be needed.

More on “Privacy Act Statement” vs. “Privacy and Security Notice”

- “Privacy Act Statement”:
  - Each Statement is unique based on collection purpose, i.e., the applicable Privacy Act System of Records.
  - Who Prepares the Statement? Data Collector/Privacy Act Officer.

- “Privacy and Security Notice”:
  - The Notice tells visitors to the web site what data elements are automatically collected.
  - Each Federal Web site must include a Notice; Notice is uniform.
  - Who Prepares the Notice? IT Staff.



- If visitor keys in his data, both a Statement and a Notice are Required.

Special Rules for Database Designers

Data Safeguards

The Privacy Act requires agencies to adopt . . .

*"appropriate **administrative**, **technical** and **physical** safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity . ."*

Data Safeguards (cont'd)

Your database must be deployed on a fully-accredited system following DODI 5200.40, DOD Information Assurance, Certification, and Accreditation Process (DIACAP) requirements.

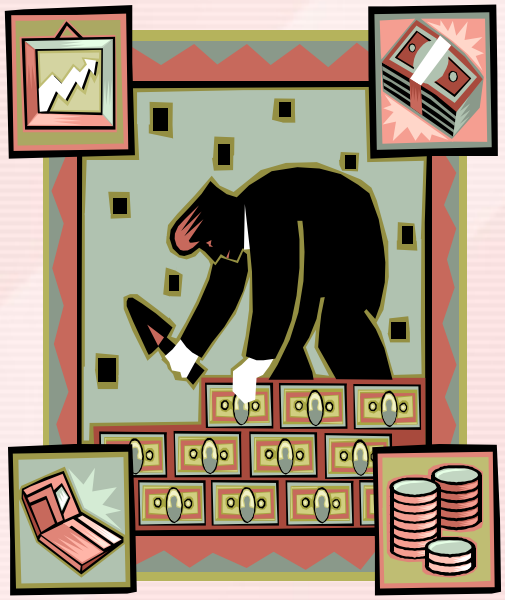
In addition to complying with computer security guidelines, your database must also meet the minimum safeguards established in:

- The governing Privacy Act System Notice.
- The governing Privacy Act Risk Assessment.
- The governing Privacy Impact Assessment (if required).

Data Safeguards (cont'd)

Build in Privacy at the Front End!

In addition to meeting the DOD IT requirements, you may want to consult the National Institute of Standards and Technology (NIST) publication, "Security Self-Assessment Guide for Information Technology Systems" (SP 800-26), which provides a checklist for safeguarding IT systems and sensitive and confidential information.



Access Limitations
The Written Consent Standard

Privacy Act Standard: No personal data may be disclosed without the written consent of the subject.

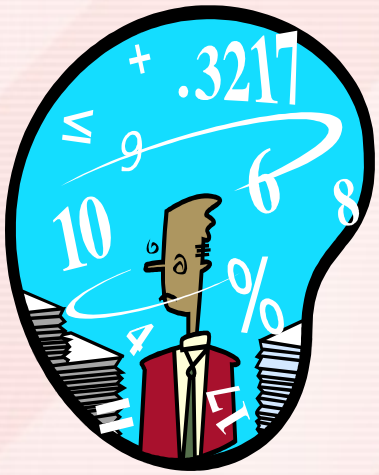
Exception to "Written Consent" Standard

- Data may be shared with those specific Federal DOD employees who need the data to perform an authorized, assigned duty

– PROVIDED –

- The data is segmented to limit access to:
  - Those specific data elements the individual needs.
- "Segmentation" rule does not apply to:
  - System Administrators
  - Privacy Act System Managers
  - Individuals who perform system maintenance or "Help Desk" functions

Surveys & Questionnaires



Surveys

OPM System Notice, OPM/GOVT-6, Personnel Research and Test Validation Records, authorizes Federal agencies to conduct surveys for personnel research.

Your survey may NOT:

- Ask participants to provide personal identifiers (names, SSNs).
- Capture and retain computer device number, email address, or other electronic identifiers.

If you will be collecting electronic identifiers, you must:

- Delete all identifiers immediately upon receipt of the survey.
- Make no attempt to link answers back to a specific person.

If you need personal identifiers because you intend to link answers back to the respondent, you must first draft a Privacy Act system notice to cover the collection. See your Privacy Act Officer before proceeding. OPM/GOVT-6 is authorized only for use with anonymous surveys.

Sample Privacy Act Advisory for a Workforce Survey

Privacy Act Advisory

Authority: Privacy Act notice OPM/GOVT-6 authorizes agencies to survey employees.

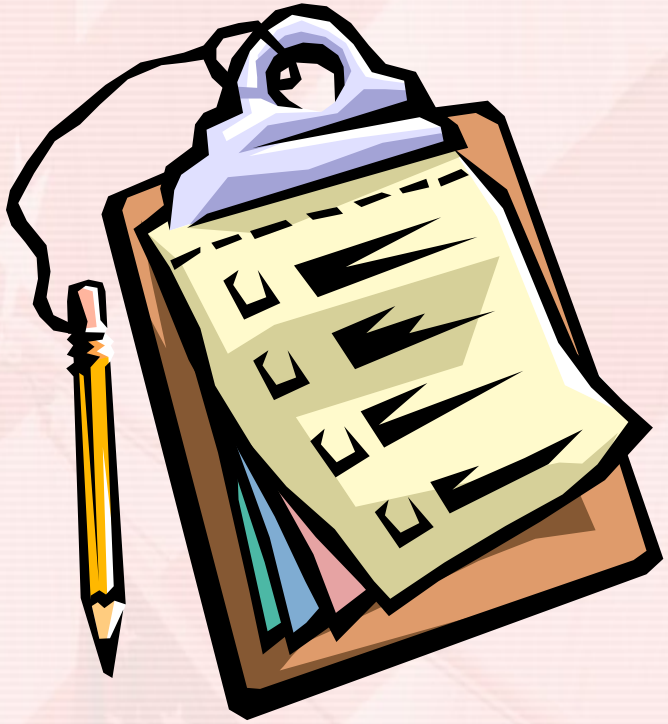
Purpose: This survey will gather data about workforce attitudes. Your input will help us decide what policies should be modified to attract a quality workforce.

Your participation is fully voluntary. If you choose not to participate, your decision will have no impact on you or your rights as an employee.

Effects of the Privacy Act: This data collection will not become part of any Privacy Act System of Record. While your computer device number will be captured as part of this survey, it will be immediately destroyed upon receipt of your response. We will not link your answers to you through your computer device number or any other personal identifier.

Survey Review: The survey questions and protocols for responding have been reviewed and approved by the HQ DLA Privacy Act Office.

Privacy Impact Assessments



The Privacy Impact Assessment (PIA)

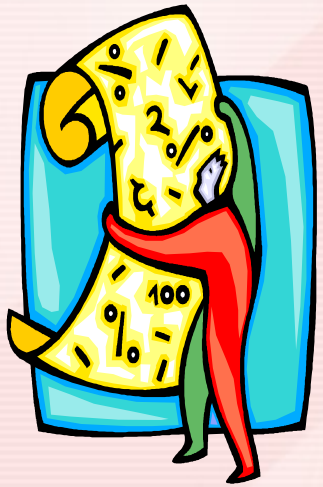
What's the Purpose of the PIA?

1. To explain to the public how we factored in privacy concerns prior to –
   - Purchasing new software
   - Designing new systems
   - Conducting new data collections

2. To assure the American public that our IT systems are being developed and used in a manner that protects and preserves personal privacy.

Privacy Impact Assessment (PIA) (cont'd)

- Source: The E-Government Act of 2002.
- Applies to: Collections of identifying data on U.S. citizens or lawful aliens.
- Does Not Apply to: Collections of identifying data on Federal civilian workers and military members.



What does the PIA Address?

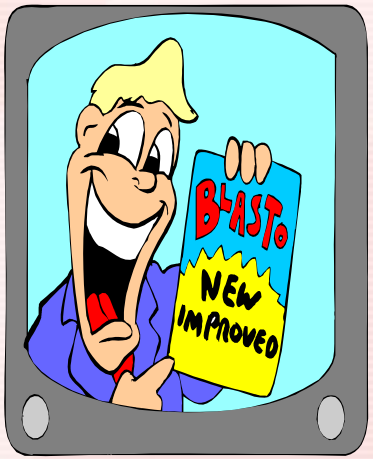
The Privacy Impact Assessment includes:

- What data is collected.
- Why the data is collected.
- How the data is used.
- How the individual objects or consents to the collection.
- How any consent is received.
- What notices will be provided to the subject regarding the collection.
- How the data will be safeguarded.
- Effects of the Privacy Act.

What Actions Might Trigger a Requirement for a PIA to be Conducted?

Whenever –

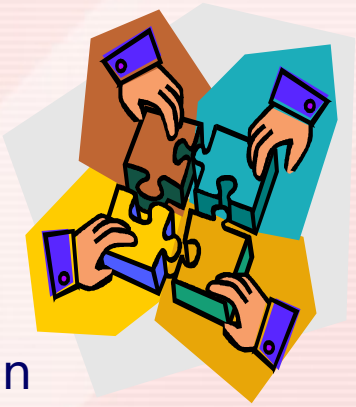
- A new system is proposed.
- An old system is changed in one or more of these ways:
  - Conversion of paper files to electronic.
  - Anonymous data becomes non-anonymous.
  - Personal data becomes more prone to exposure.
  - Two separate systems are merged.
  - Public access is newly-granted to a system.
  - A new intra- or interagency use of the data is proposed.
  - New categories of personal information are collected.



Interface: PIAs and the Privacy Act

The Privacy Act Rules Apply to:

- U.S. citizens and lawfully admitted aliens (includes military and civilian workers).
- Files retrieved by personal identifier.



The E-Government PIA Requirement Applies to:

- U. S. citizens and lawfully admitted aliens (EXCLUDED from coverage are military and civilian workers).
- All files containing data in “identifiable” form, regardless of retrieval mechanism.

What Types of Files Require PIAs & System Notices?

Type of File	PIA Needed?	Privacy Act Sys Notice Needed?
File is retrieved by personal identifier – AND –		
- Contains personal data on DOD Civ/Mil workers	NO	YES
- Contains personal data on private citizens	YES	YES
- Contains personal data on Defense Contractors	YES	YES
File is retrieved by non-personal identifier – AND –		
- Contains personal data on DOD workers	NO	NO
- Contains personal data on private citizens	YES	NO
- Contains personal data on Defense Contractors	YES	NO

Who Prepares, Signs, and Publishes the PIA?

Preparation & Web Publication:

- Data Collections Subject to the Privacy Act: The Privacy Act Officer takes the lead, collaborating with data owners, system designers, and the IT Staff.
- Non-Privacy Act Collections: The data owner or the IT Staff takes the lead in preparing and publishing the PIA.

Signature: All PIAs (Privacy Act and Non-Privacy Act) are signed by:

- The Data Owner or System Proponent.
- The Privacy Act Officer.
- The DLA Privacy Technical Advisor.
- The DLA Information Assurance Officer.
- The DLA Chief Information Officer.

If publication of the PIA raises security concerns, publish a summary only.

Remember . . .
Privacy Is Everyone's Responsibility!

For More Information, Contact:

Jody Sinkler
DLA HQ Privacy Act Officer
Defense Logistics Agency
703-767-5045
jody.sinkler@dla.mil

Or

Lew Oleinick
DLA Privacy Technical Advisor
Defense Logistics Agency
703-767-6194
lewis.oleinick@dla.mil